~~Réf~~ "Équations et variétés algébriques sur un corps fini" de J-R Joly
(Joly 72) L'ensei. math., t XIX fasc 1.2 pp 16-24

exposé le 13/10/93 (1h40)

Th. de Chevalley - Warning

Conjecturé par Artin en 1934

> " Un polynôme $P \in k[X_1, \dots, X_n]$, où $k = \mathbb{F}_q$, sans terme constant, tq $n > d$, où d = degré total de P, possède au moins 1 zéro non trivial (ie non nul) "

Démontré par Chevalley en 1935
Précisé par Warning la m̂ année.

> <u>Th. Chevalley - Warning</u> (<u>Th 1</u>)
>
> $F_1, \dots, F_s$ s polynômes de $k[X_1, \dots, X_n]$, où $k = \mathbb{F}_q$ et $q = p^f$
>
> $d_1, \dots, d_s$ degrés totaux de ces polynômes
>
> $V = \{x \in k^n \, / \, F_1(x) = \dots = F_s(x) = 0\}$
>
> $d = d_1 + \dots + d_s$
>
> Si $n > d$, alors $p \mid \#V$

<u>Rappels</u> : Posons $k[X] = k[X_1, \dots, X_n]$.

R = ens. des polynômes réduits, ie des $P \in k[X]$ de degré $\leq q-1$ en chacune des variables X_i.

I = ens. des polynômes identiquement nuls, ie tq $P(x) = 0 \ \forall x \in k^n$

Alors : 1) I et R sont des idéaux de $k[X]$, et I est l'idéal engendré par les $X_i^q - X_i$

2) En tant qu'ev. $k[X] = R \oplus I$

3) Si $F \in k[X]$, on a $F = F^* + G$ avec $F^* \in R$ et $G \in I$.
Alors $\deg F^* \leq \deg F$

<u>Idée</u> : Pour obtenir la décomposition de F dans $R \oplus I$, on remplace chaque X_i^d par

- X_i^d <u>si $d < q$</u>
- X_i^r où $d = a(q-1) + r$ et $0 \leq r < q$, <u>si $d \geq q$ et $r \neq 0$</u>
  (En effet : $X_i^d \equiv X_i^r \mod I$ dans ce cas)
- X_i^{q-1} <u>si $d \geq q$ et $q-1 \mid d$</u>
  (En effet, $X_i^d = X_i^{a(q-1)} \equiv X_i^{q-1} \mod I$, dans ce cas)

Cela prouve que $k[X] = R + I$ et le 3) ci-dessus.

<u>Preuve du Th. Ch-W</u>

Soient $F = (1 - F_1^{q-1}) \dots (1 - F_s^{q-1})$

$$F^* = \sum_{a \in V} (1 - (X_1 - a_1)^{q-1}) \dots (1 - (X_n - a_n)^{q-1})$$

F et F^* valent 1 sur V

0 sur $k^n \setminus V$

donc $G \doteq F - F^* \in I$

$$F = F^* + G \qquad F^* \in R \qquad G \in I$$

Les rappels préc. montrent que

$$\deg F^* \leq \deg F = d(q-1) < n(q-1)$$

Mais le coefficient du terme en $X_1^{q-1} \dots X_n^{q-1}$ de F^* est

$$(-1)^n \# V$$

Il devra être nul, ie $\boxed{p \mid \# V}$

Cas particulier

Toute forme quadratique $F(x)$ à n variables admet au moins un point rationnel sur k dès que $n > 2$. Géométriquement, penser aux quadriques.

Ex. de polynôme n'ayant pas de zéro dans k :

$$(X_1 + \dots + X_n)^{q-1} + 1 \qquad (\text{où } p \neq 2)$$

Thé : $F \in k[X]$, $\deg F = d$

$$d < n(q-1) \Rightarrow \sum_{x \in k^n} F(x) = 0$$

preuve : Par linéarité, on se ramène au cas où $F(X) = X_1^{u_1} \dots X_n^{u_n}$ avec $d = u_1 + \dots + u_n < n(q-1)$.

$$\sum F(x) = \sum_{x_1, \dots, x_n \in k} x_1^{u_1} \dots x_n^{u_n} = \prod_{i=1}^{n} \Big(\sum_{x_i \in k} x_i^{u_i} \Big)$$

et il existe i tq $u_i < q-1$. Il suffira de montrer :

lemme : $$\sum_{x \in k} x^u = \begin{cases} -1 & \text{si } u \neq 0 \text{ et } q-1 \mid u \\ 0 & \text{sinon} \end{cases}$$

preuve du lemme :

$$S_u \doteq \sum_{x \in k} x^u$$

* Si $u \neq 0$ et $q-1 \mid u$, $u = (q-1)v$ et

$$S_u = \sum_{x \in k} x^{(q-1)v} = q-1 = -1$$

* Si $u = 0$, $\qquad S_u = \sum_{x \in k} x^0 = q = 0 \qquad$ car $0^0 = 1$.

* Si $q-1 \nmid u$, $u = a(q-1) + r$ avec $0 < r < q-1$,
et :

$$S_u = \sum_{x \in k^*} x^{a(q-1)+r} = \sum_{x \in k^*} x^r$$

$$= \sum_{x \in k^*} (xy)^r \qquad \text{pour } y \in k^* \text{ fixé.}$$

$$= y^r S_u$$

$$(1 - y^r) S_u = 0$$

Il existe $y \in k^*$ tq $y^r \neq 1$ (prendre un générateur de k^*),
d'où $S_u = 0$

CQFD

<u>Conséquences</u> : Le Th 2 est lourd de conséquences. Il permet de démontrer le Th. de Chevalley-Warning sans passer par $k[X] = R \oplus I$ d'une part. Il est utilisé, ensuite, pour démontrer le 2^e Th. de Warning.

<u>Seconde preuve du Th. 1 utilisant le Th 2</u> :

Avec les notations du Th 1,

$$F = (1-F_1^{q-1}) \cdots (1-F_s^{q-1})$$

est de degré $d(q-1) < n(q-1)$, donc $\sum_{x \in k} F(x) = 0$,

que l'on traduit par $\sum_{a \in V} 1 = \# V = 0$. CQFD

<u>Th. 3</u> : <u>Second Th. de Warning</u>

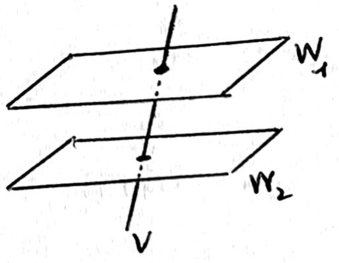
Avec les notations du Th 1.

$$\left.\begin{matrix} n > d \\ V \neq \emptyset \end{matrix}\right\} \Rightarrow q^{n-d} \leq \# V$$

preuve :

<u>lemme</u> : Si W_1, W_2 sont des sous-variétés affines de k^n parallèles et de dimension $d = d_1 + \ldots + d_s$, alors

$$\#(V \cap W_1) \equiv \#(V \cap W_2) \quad [p]$$



preuve du lemme :

On peut supposer $W_1 \neq W_2$

$$W_1 : \quad X_1 = \ldots = X_{n-d} = 0$$

$$W_2 : \quad X_1 = 1 \text{ et } X_2 = \ldots = X_{n-d} = 0$$

quitte à changer de coordonnées dans k^n.

Posons $R(T) \doteq T^{q-1}-1 = \prod_{a\in k^*}(T-a)$

$$G(X) = (-1)^{n-d} R(X_2)\dots R(X_{n-d}) \prod_{a\neq 0,1}(X_1-a)$$

On a $\deg G = (n-d-1)(q-1)+(q-2) = (n-d)(q-1)-1$

$$G(x) = \begin{cases} -1 & \text{si } x\in W_1 \\ 1 & \text{si } x\in W_2 \\ 0 & \text{ailleurs} \end{cases}$$

Notons toujours $F = (1-F_1^{q-1})\dots(1-F_s^{q-1})$

Posons $H = GF$.

$\deg H = (n-d)(q-1)-1 + d(q-1) = n(q-1)-1 < n(q-1)$

de sorte que le Th 2 s'applique :

$$\sum_{x\in k^n} H(x) = 0$$

Comme $F(x) = \begin{cases} 1 & \text{si } x\in V \\ 0 & \text{sinon} \end{cases}$, on obtient :

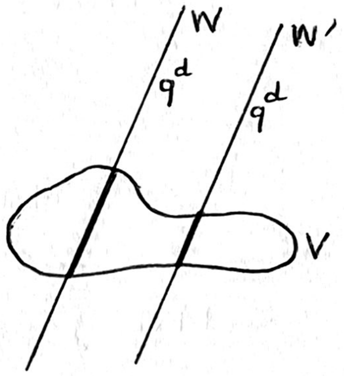
$$\sum_{x\in V\cap W_1}(-1) + \sum_{x\in V\cap W_2} 1 = 0$$

$$\# V\cap W_1 = \# V\cap W_2 \qquad (\text{dans } k)$$

CQFD

Retour à la preuve du Th 3 : on envisage 2 cas

1er cas : **$\exists$ variété aff. W de dim. d tq $\#(V \cap W) \not\equiv 0$ [p]**



Le lemme préc. montre que ce sera aussi le cas pour toute variété W' // à W.
Il existe q^{n-d} telles variétés qui contiennent chacune au moins 1 point de V, donc $\# V \geq q^{n-d}$

2e cas : **$\forall$ W variété de dim. d, on a $\#(V \cap W) \equiv 0$ [p]**

Soit $m \in \mathbb{N}_d$ défini par :

$$\begin{cases} \forall M \text{ variété de dim. } m, \ \#(M \cap V) \equiv 0 \ [p], \text{ mais } \exists L \text{ variété} \\ \text{de dim. } m-1 \text{ tq } \#(L \cap V) \not\equiv 0 \ [p] \end{cases}$$

(m existe car $V \neq \emptyset$)

Fixons L.
$\#(L \cap V) = \text{cte}.p + a$ avec $1 \leq a < p$

Combien y-a-t-il de variétés M de dim. m contenant L ?

$$\frac{q^{n-m+1} - 1}{q-1} = 1 + q + \dots + q^{n-m}$$

[En effet, on peut supposer que L est un sev de k^n. $M \supset L$ sera un sev.
Il y a bijection entre les sev M de dim m contenant L et les dtes vect. d'un supplémentaire de L dans k^n. Le nbre de dtes vect. d'un tel supplémentaire, isomorphe à $k^{n-(m-1)}$, sera $\# P_{n-m}(k)$ où $P_{n-m}(k)$ désigne l'espace projectif de dim $n-m$ sur k. On sait :

$$\# P_{n-m}(k) = \# \frac{(k^{n-m+1})^*}{\mathcal{R}} = \frac{q^{n-m+1} - 1}{q-1}$$]

On a :

$$M \cap V \supset L \cap V$$

$\# M \cap V \equiv 0 \; [p]$ $\qquad$ $\# L \cap V \equiv a \; [p]$

$1 \leq a < p$

donc $\# M \cap V \geq p \Rightarrow \# (M \setminus L) \cap V \geq p - a \geq 1$

Les $M \setminus L$ forment une partition de $k^n \setminus L$, donc

$$\# V \geq 1 + q + \cdots + q^{n-m} \geq q^{n-d}$$

CQFD

<u>Remarque finale</u> : L'inégalité du Th 3 est la meilleure possible, en ce sens

> $\forall n, d$ avec $d < n$ $\quad \exists F \in k[X]$ $\quad \deg F = d$
> et tel que $\quad \# \{ x \in k^n / F(x) = 0 \} = q^{n-d}$

preuve :

On prend un polynôme normique P de degré d, ie un polynôme $P \in k[X_1, \ldots, X_d]$ qui admet $(0, \ldots, 0)$ pour <u>seul</u> zéro dans k^n.

On pose $F(X_1, \ldots, X_n) \doteq P(X_1, \ldots, X_d)$, et :

$$F(x_1, \ldots, x_n) = 0 \iff x_1 = \cdots = x_d = 0 \quad \text{soit } q^{n-d} \text{ solutions}$$

(NB : Un tel polynôme normique existe _ Voir construction (Joly 72) p 22)